Online Safety Policy

Prepared by: The Central Team

Date: September 2025

Review: September 2026

Version: V1.1

CONTENTS

1. Introduction

Burlington House School is owned and operated by **Cavendish Education**.

In all Burlington House School policies, the words "Burlington House School" refer to Burlington House Prep, Burlington House Senior and Burlington House Sixth Form.

This policy is one of a series of school policies that, taken together, are designed to form a comprehensive statement of the school's aspiration to provide an outstanding education for each of its students and of the mechanisms and procedures in place to achieve this. Accordingly, this policy should be read alongside these policies. In particular, it should be read in conjunction with the policies covering equality and diversity, Health and Safety, safeguarding and child protection.

All of these policies have been written, not simply to meet statutory and other requirements, but to enable and evidence the work that the whole school is undertaking to ensure the implementation of its core values: that all children can achieve

While this current policy document may be referred to elsewhere in Burlington House School's documentation, including particulars of employment, it is non-contractual.

In the school's policies, unless the specific context requires otherwise, the word "parent" is used in terms of Section 576 of the Education Act 1996, which states that a 'parent', in relation to a child or young person, includes any person who is not a biological parent but who has parental responsibility, or who has care of the child. Department for Education guidance Understanding and dealing with issues relating to parental responsibility updated August 2023, considers a 'parent' to include:

- all biological parents, whether they are married or not
- any person who, although not a biological parent, has parental responsibility for a child or young person - this could be an adoptive parent, a step-parent, guardian or other relative
- any person who, although not a biological parent and does not have parental responsibility, has care of a child or young person

A person typically has care of a child or young person if they are the person with whom the child lives, either full or part-time, and who looks after the child, irrespective of what their biological or legal relationship is with the child.

The school contracts the services of third-party organisations to ensure regulatory compliance and implement best practices for:

- HR and Employment Law
- Health & Safety Guidance
- DBS Check processing
- Mandatory Safeguarding, Health & Safety, and other relevant training
- Data protection and GDPR guidance
- Specialist insurance cover

Where this policy refers to 'employees', the term refers to any individual who is classified as an employee or a worker, working with and on behalf of the school (including volunteers and contractors).

The school is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, pupils and visitors to share this commitment.

All outcomes generated by this document must take account of and seek to contribute to safeguarding and promoting the welfare of children and young people at Burlington House School.

The policy documents of Burlington House School are revised and published periodically in good faith. They are inevitably subject to revision. On occasions, a significant revision, although promulgated in school separately, may have to take effect between the republication of a set of policy documents. Care should therefore be taken to ensure, by consultation with the Senior Leadership Team, that the details of any policy document are still effectively current at a particular moment.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, disinformation, conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

The Board of Directors
The Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All Local Governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The headteacher

The headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

Details of the school's safeguarding structure, including the named designated safeguarding leads (DSL) and deputies (DDSL), are set out in our safeguarding policy, as well as relevant job descriptions.

The overall Safeguarding Lead and site-specific DSLs take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and are reviewed regularly
- Working with the Headteacher and contracted IT support provider to ensure appropriate systems and processes are in place.
- Managing all online safety issues and incidents in line with the school's safeguarding policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

<u>The ICT support provider</u>
Burlington House School contracts the services of a third-party IT support systems provider who is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting routine monitoring and security checks of the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

<u>All staff and volunteers</u>
All staff, including contractors, agency staff, and volunteers, are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the relevant DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing directly to the DSL.
- Following the correct procedures by making a request directly to the DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

<u>Parents/carers</u>
Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or the internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms of acceptable use (Appendix 2).

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. Online safety is embedded across Computing, PSHE and pastoral provision, supplemented by assemblies and workshops.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Pupils in Key Stage (KS) 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others, and know how to recognise and display respectful behaviour online, and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

In KS3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in KS4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want to be shared further, and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties, including jail
- How information and data are generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report or find support if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The Safe use of social media and the internet is reinforced through PSHE, assemblies, form time, and by staff/pupil role-modelling

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Educating parents/carers about online safety

The school shares information via the website, parent communications (e.g. Friday letter), and annual parent online safety sessions. This policy will also be made available to parents/carers through the website.

Online safety will also be covered during in-person parents' events - such as parent liaison evening.

The school will let parents/carers know:

- What systems does the school use to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the relevant DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

Definition
Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour management policy and our anti-bullying policy.)

Preventing and addressing cyber-bullying

The school addresses cyberbullying through PSHE, ICT/Computing, pastoral activities and annual parent training. Incidents are recorded in line with each site's Pastoral framework and followed up by the pastoral team, with sanctions proportionate to severity.

To help prevent cyberbullying and to support all pupils, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victims.

The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors integrate discussions of cyberbullying and online behaviour into tutor time as part of the pastoral programme.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyberbullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices
The headteacher and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- There is evidence in relation to an offence

The named staff authorised to search and confiscate electronic devices are named in the Searching, Screening and Confiscation policy.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / relevant DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

Where inappropriate material is found, the device must be reported to the DSL immediately. The DSL will decide a response in line with DfE and UKCIS guidance. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Do not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour management policy and searching, screening, and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)
Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Burlington House School recognises the educational potential and safeguarding risks of AI. Use of AI for bullying is prohibited and addressed under our Behaviour and Anti-Bullying Policy. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Burlington House School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour management policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff. Any use of Artificial Intelligence should be carried out in accordance with our AI usage policy.

8. Acceptable use of the Internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms of acceptable use if relevant.

Use of the school's internet must be for educational purposes only or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 to 3.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Pupils at the Prep and Senior sites must hand in mobile devices at morning registration. Devices may not be used during the school day. Breaches result in confiscation and sanctions under the Behaviour Policy.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour management policy, which may result in the confiscation of their device.

10. Staff using work devices outside of school

Staff must ensure work devices are password-protected, encrypted, locked when inactive, and not shared with family. Concerns must be reported to the IT support provider.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 2.

Work devices must be used solely for work activities.
If staff have any concerns over the security of their device, they must seek advice from IT support services.

11. How will the school respond to issues of misuse?

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour management and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device, where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct set out in our policies and employee manual. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

Staff, local governors and volunteers
All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example, through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and well-being issues, and children are at risk of online abuse

  Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography with those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing-type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The safeguarding team (DSLs, DDSLs) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Local Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

Pupils
All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour Management policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure(s)
- ICT and Internet Acceptable Use policy

Contact Information

For any questions or concerns regarding this policy, please contact the school's overall **Safeguarding Lead and Sixth Form DSL** - Jonathan Brophy
brophyj@burlingtonhouseschool.com

Alternatively, you may wish to contact site-specific DSLs
Burlington House **Senior** - Tim Pragnell
pragnellt@burlingtonhouseschool.com
Burlington House **Prep** - Colwin Bristol - Deputy Head (Prep)
bristolc@burlingtonhouseschool.com

Approval & Policy Review

This Policy has been reviewed and approved by:

Policy Approver(s)	Cavendish Education Board of Directors/Senior Leadership Team of the school **Localised for Burlington House School:** Jonathan Brophy
Storage Location	Online
Effective Date	September 2025
Next Review Date	September 2026

Revision History

Version	Change	Author	Date of Change
1	First published	Cavendish Central Team	July 2025
1.1	School Localisation	Adam Ford / Jonathan Brophy	September 2025

Appendix 1: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

This document is given to parents/carers electronically upon enrolment and signed via the **parent portal.**

Acceptable Use of Electronic Devices and Mobile Phone Policy

This document is issued annually. Please read it carefully with your child and then give your parental consent in the Parent Portal under the General Consents tab.

This policy relates to Burlington House Prep School and Senior School.

This document has been updated based on the following documents:

Mobile Phones in Schools - Guidance for schools on prohibiting the use of mobile phones throughout the school day (February 2024)
Prevent Duty Guidance: For England and Wales (2023)
The Prevent Duty: Departmental advice for schools and childminders (June 2015)
The use of social media online radicalisation (July 2015)

Mobile Phones

- Pupils are discouraged from bringing phones/ electronic items to school. Parents are informed that these items are not insured through the school's policy and thus parents are responsible for independent insurance.
- All pupil mobile phones and other electronic devices such as ipads, game consoles, smart watches etc, that are brought to school, must be handed to Prep Reception or Senior Form Tutors/ LSAs at morning registration. They will be returned at the end of the day.
- Mobile phones must not be used by pupils on the school premises, including before morning registration and after pm registration. Failure to comply may result in the device being confiscated for up to 1 week and parents asked to collect (please see Behaviour Management policy). A member of the Leadership Team will phone home to inform parents of the sanction.
- All pupils follow teachers' instructions fully regarding phone use on school trips/ external activities and use their mobile phones responsibly when allowed to do so.
- Pupils are taught the risks that are associated with the use of mobile phones, in Form time, PSHE lessons and in whole school gatherings, to ensure they understand the reasons for the school's policy.

Acceptable Use of Electronic Devices issued by the School:

Laptops and Storage Devices

- To only use the school laptop that you were given by the school
- To store your laptop in the secure designated places when not in use
- To not modify or change your laptop
- To inform your form tutor when your laptop is not working correctly
- To transport your laptop in a safe manner
- To refrain from using all electronic devices during breaks

Network Accounts / Profiles

- To only access your personal network account
- To not share your password
- To store only suitable digital content on your personal profile
- To only used authorised software programs
- To not hack or attempt to hack into unauthorised areas of the network.
- To not to attempt to spread viruses via the network.
- To not attempt to bypass the schools security system

Email

- To use appropriate language in all email messages
- To attach appropriate images and links in all email messages
- To never access any other pupils email account
- To inform staff if you observe another pupil inappropriately using email
- Not to open attachments coming from an unknown sender
- Not to use email in lessons unless instructed by a teacher

Websites

- To use only websites and games that contain appropriate content. To help you with this, any inappropriate content will be blocked by our Smoothwall.
- To inform staff if you observe another pupil on inappropriate websites or games (containing adult content, extremist or terrorist content)
- To follow teacher instructions immediately in respect to the use of the Internet at anytime
- To close the Web Browser when instructed to by a staff member
- To not use school computers or mobile devices for any form of illegal activity, including software and music piracy

Screen Free Breaks

All pupils will refrain from using electronic devices (including their school laptop) during Breaks, unless specific permission is given by a teacher.

Agreement of Acceptable Use of Electronic Devices and Mobile Phone Policy

"I understand and agree to the Acceptable Use of Electronic Devices at Burlington House School."

Please read this document carefully with your child and then select the option "Consent given".

KS5 Sixth Form acceptable use agreement (pupils and parents/carers)

This document is given to parents/carers electronically upon enrolment and signed via the **parent portal.**

Acceptable Use of Electronic Devices and Mobile Phone Policy

This document is issued annually. Please read it carefully with your child and then give your parental consent in the Parent Portal under the General Consents tab.

This policy relates to Burlington House Prep School and Senior School.

This document has been updated based on the following documents:

Mobile Phones in Schools - Guidance for schools on prohibiting the use of mobile phones throughout the school day (February 2024)
Prevent Duty Guidance: For England and Wales (2023)
The Prevent Duty: Departmental advice for schools and childminders (June 2015)
The use of social media online radicalisation (July 2015)

Mobile Phones

- Pupils are discouraged from bringing phones/ electronic items to school. Parents are informed that these items are not insured through the school's policy and thus parents are responsible for independent insurance.
- All pupil mobile phones and other electronic devices such as ipads, game consoles, smart watches etc, that are brought to school are at their own risk and students are encouraged to put any valuables in their lockers.
- Mobile phones must not be used by pupils in lessons unless permission has been given by the classroom teacher. Any pupil who makes use of their phone without permission is given a warning at first and it is then confiscated upon the second incident. The phone is given to reception and the pupil can only collect at the end of the Sixth Form school day.
- All pupils follow teachers' instructions fully regarding phone use on school trips/ external activities and use their mobile phones responsibly when allowed to do so.
- Pupils are taught the risks that are associated with the use of mobile phones, in Form time, PSHE lessons and in whole school gatherings, to ensure they understand the reasons for the school's policy.
- Any activity on a school device or using a school network is monitored and emails made through a school account may be read by a relevant member of staff when needed.

Acceptable Use of Electronic Devices issued by the School:

Laptops and Storage Devices

- To only use the school laptop that you were given by the school
- To store your laptop in the secure designated places when not in use
- To not modify or change your laptop
- To inform your form tutor when your laptop is not working correctly
- To transport your laptop in a safe manner

Network Accounts / Profiles

- To only access your personal network account
- To not share your password
- To store only suitable digital content on your personal profile
- To only use authorised software programs
- To not hack or attempt to hack into unauthorised areas of the network.
- To never attempt to spread viruses via the network.
- To not attempt to bypass the schools security system

Email

- To use appropriate language in all email messages
- To attach appropriate images and links in all email messages
- To never access any other pupils email account
- To inform staff if you observe another pupil inappropriately using email
- Not to open attachments coming from an unknown sender
- Not to use email in lessons unless instructed by a teacher

Websites

- To use only websites and games that contain appropriate content. To help you with this, any inappropriate content will be blocked by our Smoothwall.
- To inform staff if you observe another pupil on inappropriate websites or games (containing adult content, extremist or terrorist content)
- To follow teacher instructions immediately in respect to the use of the Internet at anytime
- To close the Web Browser when instructed to by a staff member
- To not use school computers or mobile devices for any form of illegal activity, including software and music piracy

Agreement of Acceptable Use of Electronic Devices and Mobile Phone Policy

"I understand and agree to the Acceptable Use of Electronic Devices at Burlington House School."

Please read this document carefully with your child and then select the option "Consent given".

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Please see the full Policy - Acceptable Use Agreement (Staff) - 2024 Edition

Appendix 3: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident